BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

Cryptographic method and cryptographic device

Patent number:	DE10024325
Publication date:	2001-12-06
Inventor:	SEYSEN MARTIN (DE)
Applicant:	GIESECKE & DEVRIENT GMBH (DE)
Classification:	
- international:	H04L9/30
- european:	G06F7/72E
Application number:	DE20001024325 20000517
Priority number(s):	DE20001024325 20000517

Also published as:

W O0188693 (A3)
W O0188693 (A2)
US 2004028221 (A1)

Abstract not available for DE10024325
Abstract of correspondent: **US2004028221**

The invention relates to a cryptographic method with at least one computing step containing a modular exponentiation E according to E=x<d >(mod p.q), with a first prime factor p, a second prime factor q, an exponent d and a number x, whereby the modular exponentiation E is calculated according to the Chinese Remainder Theorem.

---

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 100 24 325 A 1**

(51) Int. Cl.[7]: H 04 L 9/30

(21) Aktenzeichen: 100 24 325.8
(22) Anmeldetag: 17. 5. 2000
(43) Offenlegungstag: 6. 12. 2001

DE 100 24 325 A 1

(71) Anmelder:
Giesecke & Devrient GmbH, 81677 München, DE

(72) Erfinder:
Seysen, Martin, Dr., 80809 München, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Kryptographisches Verfahren und kryptographische Vorrichtung

(57) Die Erfindung betrifft ein kryptographisches Verfahren mit mindestens einem eine modulare Exponentiation E gemäß $E = x^d \pmod{p \cdot q}$ enthaltenden Rechenschritt mit einem ersten Primfaktor p, einem zweiten Primfaktor q, einem Exponenten d und einer Zahl x, wobei die modulare Exponentiation E gemäß dem Chinesischen Restwertsatz berechnet wird.

DE 100 24 325 A 1

Beschreibung

[0001] Kryptographische Verfahren in Gestalt von Verschlüsselungs- und Signaturverfahren erfreuen sich insbesondere durch die steigende Bedeutung des elektronischen Geschäftsverkehres einer stetig wachsenden Verbreitung. Sie werden in der Regel mittels elektronischer Vorrichtungen implementiert, die beispielsweise einen programmierbaren universellen Microkontroller oder auch eine spezialisierte elektronische Schaltung etwa in Gestalt eines ASIC beinhalten können. Eine besonders interessante Form kryptographischer Vorrichtungen ist die Chipkarte, da sich in ihr bei zweckdienlicher technischer Ausgestaltung geheime Schlüsseldaten gegen unbefugten Zugriff schützen lassen. Ein ständiges Bemühen gilt dabei sowohl der Verbesserung der Ausführungsgeschwindigkeit der kryptographischen Verfahren als auch deren Sicherung gegen alle denkbaren Arten von Angriffen. Die Erfindung eignet sich insbesondere für den Einsatz im Zusammenhang mit Chipkarten, ist aber in keiner Weise darauf beschränkt. Sie ist vielmehr im Zusammenhang mit allen Arten von kryptographischen Vorrichtungen implementierbar.

[0002] Bei einer Reihe bekannter kryptographischer Verfahren ist es erforderlich, eine modulare Exponentiation gemäß der Gleichung

$$E = x^d(\text{mod } N) = x^d(\text{mod } p \cdot q) \quad (1)$$

durchzuführen, wobei p und q Primzahlen sind. Ein besonders bedeutendes kryptographisches Verfahren, welches einen modularen Exponentiationsschritt beinhaltet, ist das beispielsweise aus Alfred J. Menezes, Paul C. von Oorschot und Scott A. Vanstone, "Handbook of Applied Cryptography", Boca Raton: CRC Press, 1997, Seiten 285 bis 291, bekannte RSA-Verfahren. Die Verwendung der modularen Exponentiation ist jedoch nicht auf das RSA-Verfahren beschränkt, sondern umfaßt beispielsweise auch aus Menezes et al., a. a. O., Seiten 438 bis 442, bekannte Rabin-Signaturen und das aus Menezes et al., a. a. O., Seite 408 bis 410, bekannte Fiat-Shamir'sche Identifikationsschema.

[0003] Die Sicherheit von kryptographischen Verfahren, die die modulare Exponentiation einbeziehen, ist regelmäßig abhängig von der Schwierigkeit, die Zahl N aus Gleichung (1) in ihre Primfaktoren p und q zerlegen zu können. Dieses Problem ist nur für hinreichend große Werte N von ausreichender Komplexität, so daß einerseits N möglichst groß gewählt werden sollte. Der Rechenaufwand zur Berechnung von Werten mittels modularer Exponentiation gemäß Gleichung (1) steigt andererseits monoton mit der Größenordnung von N, so daß es unter dem Gesichtspunkt der praktischen Anwendbarkeit wünschenswert wäre, trotz großer Werte von N den Rechenzeitaufwand auf akzeptable Werte beschränken zu können.

[0004] Es ist bekannt, durch Anwendung des sog. "Chinesischen Restwertsatzes" die Rechengeschwindigkeit um einen Faktor 4 erhöhen zu können, wodurch beispielsweise bei gleicher Rechenzeit größere Werte N zugelassen werden können. Statt unmittelbar die Gleichung (1) auszuwerten, wird eine Umformung vorgenommen gemäß

$$E = x^d(\text{mod } p \cdot q) = aE_1 + bE_2(\text{mod } N) \quad (2)$$

mit

$$E_1 = x^d(\text{mod } p) \quad (3)$$

$$E_2 = x^d(\text{mod } q) \quad (4)$$

[0005] Eine Folge der Anwendung des Chinesischen Restwertsatzes besteht darin, daß die modulare Exponentiation nicht mehr modulo N, also modulo derjenigen Zahl, die ihre eigene Primfaktorzerlegung noch in sich verbirgt, sondern nacheinander in einem ersten Teilschritt modulo p und in einem zweiten Teilschritt modulo q erfolgt, d. h. die Kenntnis der geheimzuhaltenden Primfaktorzerlegung $n = p \cdot q$ wird bei dieser Rechenvorschrift vorausgesetzt und führt zu einer Aufteilung des Gesamtrechenprozesses in einen ersten Rechenschritt (3), in den der erste Primfaktor wesentlich eingeht, und einen zweiten Rechenschritt (4), in den der zweite Primfaktor wesentlich eingeht. Der Vorteil hierbei liegt darin, daß der Exponent d in Gleichung (1) modulo $\phi(p \cdot q)$ definiert sein muß, wohingegen die Exponenten in Gleichung (2) lediglich $\phi(p)$ bzw. $\phi(q)$ definiert sein müssen, wobei mit ϕ die Euler'sche Funktion notiert ist.

[0006] Interessanterweise ist nun in der letzten Zeit ein Angriffsschema auf solche kryptographischen Verfahren, die die modulare Exponentiation nutzen, bekannt geworden, bei dem durch einen geeigneten artifiziellen Eingriff in den ansonsten störungsfreien Rechenablauf aus dem fehlerhaften Ergebnis einer gestörten modularen Exponentiation die Information über die Primfaktorzerlegung von N zurückgewonnen werden kann, sofern die konkrete Implementation von dem Chinesischen Restwertsatz gemäß den Gleichungen (2) bis (4) Gebrauch macht. Dieser als "Bellcore-Angriff" bekannte Versuch ist beispielsweise in Dan Boneh, Richard A. DeMillo und Richard J. Lipton: "On the importance of checking Cryptographic Protocols for Faults" Advances in Cryptology-EUROCRYPT, 97, Lecture Notes in Computer Science 1233, Berlin: Springer, 1997 beschrieben. Eine Verschlüsselungseinrichtung wird durch physikalische Eingriffe wie beispielsweise Übertaktung, zu hohe Betriebsspannung oder Bestrahlung manipuliert, so daß mit einer gewissen, nicht zu großen Wahrscheinlichkeit Rechenfehler bei der Ausführung der modularen Exponentiation nach dem Chinesischen Restwertsatz auftreten. Wenn ein Rechenfehler nur bei einem der beiden Terme in Gleichung (2) auftritt, können die beiden Primfaktoren p und q aus dem fehlerbehafteten Exponentiationsergebnis rekonstruiert werden.

[0007] Die aus dieser Verletzlichkeit der mittels des Chinesischen Restwertsatzes implementierten modularen Exponentiation zu ziehende Konsequenz besteht darin, das Ergebnis des Rechenvorganges zuerst auf seine Korrektheit zu prüfen, bevor es weiterverarbeitet, insbesondere aber bevor es in irgend einer Form, etwa in Gestalt einer Signatur, ausgegeben wird.

[0008] Ein triviales Gegenmittel gegen den "Bellcore-Angriff" besteht darin, diese Korrektheitsprüfung dadurch zu bewerkstelligen, indem der Rechenvorgang mindestens einmal wiederholt wird. Bei zufälligen Rechenfehlern kann davon ausgegangen werden, daß das Ergebnis des ersten Rechenganges von demjenigen der Kontrollrechengänge abweicht. Der wesentliche Nachteil dieses Ansatzes besteht darin, daß sich die Rechenzeit bereits bei einer Kontrollrechnung verdoppelt.

[0009] Aus der Druckschrift WO-A1-98/52319 ist insbesondere ein Verfahren zum Schutz von eine modulare Exponentiation nach dem Chinesischen Restwertsatz ausführenden Rechenoperationen gegen den "Bellcore-Angriff" bekannt. Dabei werden zwei geheime ganze Zahlen j_1 und j_2 beispielsweise im Bereich $[0, 2^k - 1]$ mit $16 \leq k \leq 32$ ausgewählt. Sodann werden folgende Ausdrücke berechnet:

$$v_1 = x(\text{mod } j \cdot q) \quad (5)$$

$$v_2 = x(\text{mod } j \cdot q) \quad (6)$$

$d_1 = d(\mathrm{mod}\ \phi(j \cdot p))$ (7)

$d_2 = d(\mathrm{mod}\ \phi(j \cdot q))$ (8)

$w_1 = v_1^{d1}(\mathrm{mod}\ j \cdot p)$ (9)

$w_2 = v_2^{d2}(\mathrm{mod}\ j \cdot q)$ (10)

Sodann wird geprüft, ob gilt:

$w_1 = w_2(\mathrm{mod}\ j)$ (11)

[0010] Kann der Ausdrucke (11) verifiziert werden, so werden bei dem bekannten Verfahren folgende Ausdrücke berechnet:

$y_1 = w_1(\mathrm{mod}\ p)$ (12)

$y_2 = w_2(\mathrm{mod}\ q)$ (13)

woraus dann mittels des Chinesischen Restwertsatzes der Wert für

$E = x^d(\mathrm{mod}\ N)$ (14)

ermittelt werden kann.

[0011] Dieses bekannte Verfahren weist gegenüber einfachen Kontrollrechengängen den Vorteil auf, daß der zusätzliche Rechenzeitaufwand wesentlich geringer ist.

[0012] Bei diesem Verfahren müssen beide Primzahlen p und q mit demselben Faktor d multipliziert werden. In der Druckschrift WO-A1-98/52319 ist ein zweites Verfahren beschrieben, welches es erlaubt, die Primzahlen p und q mit verschiedenen Faktoren r und s zu multiplizieren. Hierbei sind jedoch für die Kontrollrechnung zwei weitere Exponentiationen möglich.

[0013] Aufgabe der Erfindung ist es, ein kryptographisches Verfahren bzw. eine kryptographische Vorrichtung anzugeben, bei dem bzw. bei der unter Beibehaltung oder Erhöhung der Sicherheit Rechenoperationen oder Rechenzeit eingespart werden kann.

[0014] Diese Aufgabe wird erfindungsgemäß gelöst durch ein kryptographisches Verfahren mit den in Anspruch 1 oder 2 angegebenen Merkmalen als auch durch eine kryptographische Vorrichtung mit den in Anspruch 13 oder 14 angegebenen Merkmalen.

[0015] Den abhängigen Ansprüchen 3 bis 12 sowie 15 bis 24 sind vorteilhafte Weiterbildungen entnehmbar.

[0016] Wie weiter unten erwähnt wird, ist es auf bestimmten Rechenwerken vorteilhaft, wenn ein Modulus bei der modularen Exponentiation viele führende binäre Einsen besitzt, so daß verschiedene Faktoren r und s hier einen gewissen Vorteil bedeuten. Ferner gibt es für die modulare Exponentiation optimierte Rechenwerke, wobei aber allein der Datentransfer von der Zentraleinheit in das optimierte Rechenwerk für die Exponentiation einen beträchtlichen Verwaltungsaufwand verursacht. Die vorliegende Erfindung spart gegenüber dem oben beschriebenen Verfahren bei verschiedenen Faktoren r und s eine Exponentiation ein.

[0017] Erfindungsgemäß werden zwei ganze Zahlen r und s beispielsweise im Bereich $[0, 2^k - 1]$ mit $16 \leq k \leq 32$ ausgewählt, so daß d teilerfremd zu $\phi(\mathrm{lcm}(r,s))$ ist, wobei lcm(r,s) das kleinste gemeinsame Vielfache von r und s angibt, und $\phi()$ die Euler'sche Funktion darstellt. Sodann werden folgende Ausdrücke berechnet:

$x_1 = x(\mathrm{mod}\ p \cdot r)$ (15)

$x_2 = x(\mathrm{mod}\ q \cdot s)$ (16)

$d\_1 = d(\mathrm{mod}\ \phi(p \cdot r))$ (15)

$d\_2 = d(\mathrm{mod}\ \phi(q \cdot s))$ (16)

$z_1 + x_1^{d\_1}(\mathrm{mod}\ p \cdot r)$ (15)

$z_2 = x_2^{d\_2}(\mathrm{mod}\ q \cdot s)$ (16)

[0018] Jetzt gilt $z_1 = x^d(\mathrm{mod}\ p \cdot r)$ und $z_2 = x^d(\mathrm{mod}\ q \cdot s)$. Nach dem Chinesischen Restwertsatz läßt sich aus z_1 und z_2 leicht eine Zahl z berechnen mit

$z = z_1(\mathrm{mod}\ p \cdot r);\ z = z_2(\mathrm{mod}\ q \cdot s);\ z = x^d(\mathrm{mod}\ p \cdot q \cdot \mathrm{lcm}(r,s))$ (17)

[0019] Die Zahlen r und s müssen erfindungsgemäß so gewählt werden, daß d teilerfremd ist zu $\phi(\mathrm{lcm}(r,s))$. Unter diesen Umständen läßt sich mit Hilfe des erweiterten Euklid'schen Algorithmus leicht eine natürliche Zahl e finden mit

$e \cdot d = 1(\mathrm{mod}\ \phi(\mathrm{lcm}(r,s)))$ (18)

[0020] Mit Hilfe von Z und e wird die Zahl C wie folgt berechnet:

$C = z^e(\mathrm{mod}\ \mathrm{lcm}(r,s))$ (19)

[0021] Nach dem Fermat'schen Satz gilt:

$C = x^{d \cdot e} = x(\mathrm{mod}\ \mathrm{lcm}(r,s))$ (20)

[0022] Durch Vergleich der beiden Werte C und x modulo lcm(r,s) läßt sich ein Fehler mit hoher Wahrscheinlichkeit feststellen. Wenn $C \neq x\ (\mathrm{mod}\ \mathrm{lcm}(r,s))$ festgestellt wird, ist das Ergebnis der modularen Exponentiation als fehlerbehaftet anzusehen und zu verwerfen.

[0023] Bei RSA-Verfahren (ebenso wie beim Rabin'schen Signaturverfahren) ist zur Erzeugung einer digitalen Signatur oder zur Entschlüsselung eine modulare Exponentiation durchzuführen, wobei der Modulus $p \cdot q$ und Exponent d nur vom privaten Schlüssel abhängen. Infolgedessen können die Zahlen d, e, r und s einmal beim Einbringen des privaten Schlüssel berechnet und zur Wiederverwendung abgespeichert werden.

[0024] In einer Variante der Erfindung werden ebenfalls zwei ganze Zahlen r und s beispielsweise im Bereich $[0, 2^k - 1]$ mit $16 \leq k \leq 32$ ausgewählt. Auf einem binären Rechenwerk wird empfohlen, daß die Zahlen r und s beide ungerade sind. Außerdem werden zwei feste, nicht von x abhängige Zahlen b_1 und b_2 im Intervall $[1, \ldots, r-1]$ bzw. $[1, \ldots, s-1]$ und teilerfremd zu r bzw. s gewählt. Falls r und s nicht teilerfremd sind, müssen b_1 und b_2 die zusätzliche Bedingung $b_1 = b_2\ (\mathrm{mod}\ \mathrm{ggt}(r,s))$ erfüllen, wobei ggt(r,s) den größten gemeinsamen Teiler von r und s bezeichnet.

[0025] Nach dem Chinesischen Restsatz wird zunächst eine Zahl x_1 berechnet mit

$x_1 = x(\mathrm{mod}\ p),\ x_1 = b_1(\mathrm{mod}\ r)$ (21)

[0026] Ebenso wird eine Zahl x_2 berechnet mit

$x_2 = x(\mathrm{mod}\ q),\ x_2 = b_2(\mathrm{mod}\ s)$ (22)

[0027] Sodann werden folgende Ausdrücke berechnet:

$$d\_1 = d(\mathrm{mod}\ \phi(p)) \quad (23)$$

$$d\_2 = d(\mathrm{mod}\ \phi(q)) \quad (24)$$

$$z_1 = x_1^{d\_1}(\mathrm{mod}\ p \cdot r) \quad (25)$$

$$z_2 = x_2^{d\_2}(\mathrm{mod}\ q \cdot s) \quad (26)$$

$$C_1 = b_1^{d\_1}(\mathrm{mod} \cdot r) \quad (27)$$

$$C_2 = b_2^{d\_2}(\mathrm{mod} \cdot s) \quad (28)$$

[0028] Zur Einsparung von Rechenzeit können die Exponenten d_1 und d_2 in (27) bzw. (28) vor der Durchführung der Exponentiation modulo $\phi(r)$ bzw. $\phi(s)$ reduziert werden.

[0029] Aus (23) und (25) folgt

$$z_1 = x^d(\mathrm{mod}\ p) \quad (29)$$

[0030] Aus (24) und (26) folgt

$$z_2 = x^d(\mathrm{mod}\ q). \quad (30)$$

[0031] Nach dem Chinesischen Restwertsatz läßt sich aus z_1 und z_2 leicht eine Zahl z berechnen mit

$$z = z_1(\mathrm{mod}\ p \cdot r);\ z = z_2(\mathrm{mod}\ q \cdot s); \quad (31)$$

[0032] Selbst wenn r und s nicht teilerfremd sind, existiert eine solche Zahl z wegen $z_1 = C_1 = b_1^{d\_1} = b_2^{d\_2} = C_2 = z_2(\mathrm{mod}\ \gcd(r,s))$. Da p und q teilerfremd sind, folgt aus (29), (30) und (31):

$$z = x^d(\mathrm{mod}\ p \cdot q). \quad (32)$$

so daß sich die gesuchte Zahl z leicht aus den oben berechneten Werten ermitteln läßt.

[0033] Aus (21), (25) und (27) folgt

$$z_1 = C_1(\mathrm{mod}\ r) \quad (33)$$

[0034] Aus (22), (26) und (28) folgt

$$z_2 = C_2(\mathrm{mod}\ s). \quad (34)$$

[0035] Durch Prüfung der Bedingungen (33) und (34) läßt sich ein Fehler mit hoher Wahrscheinlichkeit feststellen. Wenn eine der Bedingungen (33) oder (34) verletzt wird, ist das Ergebnis der modularen Exponentiation als fehlerbehaftet anzusehen und zu verwerfen.

[0036] Im Gegensatz zu dem Verfahren in Patentanspruch 8 der Druckschrift WO-A1-98/52319 sind die Zahlen b_1 und b_2 in bei dem hier vorgestellten Variante des Verfahrens nicht von der Basis x abhängig. Typischerweise wird bei der Anwendung des RSA-Verfahrens oder des Rabin'schen Signaturverfahrens ein privater Schlüssel einmal in ein kryptographisches Gerät, z. B. in eine Chipkarte eingebracht, und anschließend mehrmals verwendet. Hierbei ist bei der in diesen Verfahren angewendeten modularen Exponentiation der Exponent d sowie der Modulus p · q jeweils ein fester Bestandteil des privaten Schlüssels. Infolgedessen müssen daß die Werte C_1 und C_2 nur einmal beim Einbringen des Schlüssels in das kryptographische Gerät berechnet werden, und können dann anschließend in dem Gerät abgespeichert werden. Das Abspeichern dieser Werte spart ggü. dem in der Druckschrift WO-A1-98/52319 vorgestellten Verfahren zwei modulare Exponentiationen.

[0037] Eine kryptographische Vorrichtung, beispielsweise eine Chipkarte, mit einer Zusatzhardware für die Beschleunigung der modularen Arithmetik enthält bei üblichen Ausführungsformen schnelle Addier- und/oder Multiplizierein-heiten, während die bei er modularen Reduktion erforderliche Division durch eine lange Zahl nach üblichen Standardverfahren durchgeführt werden muß, wie sie beispielsweise aus Donald Knuth: "The Art of Computer Programming", Volume 2: Seminumerical Algorithms, 2. Ed., Addison-Wesley, 1981, bekannt sind. Eines von mehreren bekannten Verfahren zur Vereinfachung der Divisionsoperation besteht darin, den Modulus p vor der Exponentiation mit einer Zahl r zu multiplizieren, so daß die Binärdarstellung des Produktes p · r möglichst viele Einsen enthält; siehe beispielsweise Menezes et al. a. a. O., Seiten 598 bis 599. Die Division durch eine Zahl mit möglichst vielen führenden Einsen ist erheblich einfacher als die Division durch eine allgemeine Zahl.

[0038] Der Multiplikator r wird erfindungsgemäß so gewählt, daß d teilerfremd zu $\phi(r)$ ist. Für jeden Modulus p gibt es einen von der jeweiligen technischen Implementierung der Division abhängigen optimalen Multiplikator r_{opt}. Falls der gewählte Wert von r geringfügig kleiner als das Optimum ist, enthält das Produkt p · r immer noch genügend viele führende Einsen, um die Division einfach gestalten zu können. Mit hoher Wahrscheinlichkeit ist die Zahl d teilerfremd zu mindestens einem der Werte $\phi(r_{opt} - i)$, wobei i = 1, . . ., k, wobei k eine von der Implementation abhängige kleine Zahl ist.

[0039] Wenn dies nicht der Fall ist, ersetze man r durch $2^i \cdot r$, wobei 2^i eine von der Implementierung abhängige geeignete Zweierpotenz ist.

[0040] Dieselben Substitutionen sind entsprechend auch auf den zweiten Primfaktor q anwendbar. Da die Multiplikatoren r (für p) und s (für q) unabhängig voneinander gewählt werden können, ist für den Multiplikator s ebenfalls eine entsprechende Wahl möglich.

Patentansprüche

1. Kryptographisches Verfahren,
   a) mit mindestens einem eine modulare Exponentiation E

   $$E = x^d(\mathrm{mod}\ p \cdot q)$$

   enthaltenden Rechenschritt mit einem ersten Primfaktor p, einem zweiten Primfaktor q, einem Exponenten d und einer Basis x, wobei
   b) zur Durchführung der modularen Exponentiation zwei natürliche Zahlen r und s gewählt werden mit der Bedingung, daß d teilerfremd ist zu $\phi(\mathrm{lcm}(r,s))$ und wobei die folgenden Rechenschritte durchgeführt werden:

   $$x_1 = x(\mathrm{mod}\ p \cdot r)$$

   $$x_2 = x(\mathrm{mod}\ q \cdot s)$$

   $$d\_1 = d(\mathrm{mod}\ (p \cdot r))$$

   $$d\_2 = d(\mathrm{mod}\ \phi(q \cdot s))$$

   $$z_1 = x_1^{d\_1}(\mathrm{mod}\ p \cdot r)$$

   $$z_2 = x_2^{d\_2}(\mathrm{mod}\ q \cdot s),$$

   und wobei $\phi(.)$ die Euler'sche Funktion und

lcm(r,s) das kleinste gemeinsame Vielfache von r und s darstellt,

c) anschließend nach dem Chinesischen Restwertsatz aus z_1 und z_2 eine Zahl z berechnet wird mit $z = z_1 \pmod{p \cdot r}$; $z = z_2 \pmod{q \cdot s}$;

d) das Ergebnis E der Exponentiation durch Reduktion von z modulo $p \cdot q$ berechnet wird

e) die vorher berechnete Zahl z und damit das Ergebnis E in einem Prüfschritt auf Rechenfehler geprüft wird,

f) der Prüfschritt folgende Rechenoperationen beinhaltet:

f1) Berechnen der kleinstmöglichen natürlichen Zahl e mit der Eigenschaft $e \cdot d = 1 \pmod{\phi(\text{lcm}(r,s))}$ mit Hilfe des erweiterten Euklids'schen Algorithmus

f2) Berechnen des Wertes $C = z^e \pmod{\text{lcm}(r,s)}$

f3) Vergleich der Werte x und C modulo lcm(r,s), wobei das Ergebnis der modularen Exponentiation E als fehlerhaft verworfen wird, wenn $x \neq C \pmod{\text{lcm}(r,s)}$.

2. Kryptographisches Verfahren,

a) mit mindestens einer eine modulare Exponentiation E

$$E = x^d \pmod{p \cdot q}$$

enthaltenden Rechenschritt mit einem ersten Primfaktor p, einem zweiten Primfaktor q, einem Exponenten d und einer Basis x, wobei

b) zur Durchführung der modularen Exponentiation zwei natürliche Zahlen r und s, sowie zwei Zahlen b_1 und b_2 im Intervall $[1, \ldots, r-1]$ bzw. $[1, \ldots, s-1]$ und teilerfremd zu r bzw. s gewählt werden, und wobei b_1 und b_2 die Bedingung $b_1 = b_2 \pmod{\text{ggt}(r,s)}$ erfüllen, wobei ggt(r,s) den größten gemeinsamen Teiler von r und s bezeichnet,

c) mit Hilfe dir beiden Zahlen b_1 und b_2 nach dem Chinesischen Restwertsatz Werte x_1 und x_2 berechnet werden, die die folgenden Bedingungen erfüllen:

$$x_1 = x \pmod{p},\ x_1 = b_1 \pmod{r}$$

$$x_2 = x \pmod{q},\ x_2 = b_2 \pmod{s}$$

und anschließend folgende Rechenschritte durchgeführt werden:

$$d\_1 = d \pmod{\phi(p)}$$

$$d\_2 = d \pmod{\phi(q)}$$

$$z_1 = x_1^{d\_1} \pmod{p \cdot r}$$

$$z_2 = x_2^{d\_2} \pmod{q \cdot s}$$

und $\phi(.)$ die Euler'sche Funktion und lcm(r,s) das kleinste gemeinsame Vielfache von r und s darstellt,

d) anschließend nach dem Chinesischen Restwertsatz aus z_1 und z_2 eine Zahl z berechnet wird mit $z = z_1 \pmod{p \cdot r}$; $z = z_2 \pmod{q \cdot s}$

e) das Ergebnis E der Exponentiation durch Reduktion von z modulo $p \cdot q$ berechnet wird

f) die vorher berechnete Zahl z (und damit automatisch auch das Ergebnis E) in einem Prüfschritt auf Rechenfehler geprüft wird,

g) der Prüfschritt folgende Rechenoperationen beinhaltet:

g1) Berechnen der Zahlen

$$C_1 = b_1^{d\_1} \pmod{r}$$

$$C_2 = b_2^{d\_2} \pmod{s}$$

wobei d_1 und d_2 vor der Durchführung der modularen Exponentiation modulo $\phi(r)$ bzw. $\phi(s)$ reduziert werden

g2) Vergleich der Werte z_1 und C_1 modulo r sowie z_2 und C_2 modulo s, wobei das Ergebnis der modularen Exponentiation E als fehlerhaft verworfen wird, wenn $C_1 \neq z_1 \bmod r$ oder $C_2 \neq z_2 \bmod s$ gilt.

3. Kryptographisches Verfahren nach Anspruch 2, dadurch gekennzeichnet, daß die Zahlen r und s ungerade sind.

4. Kryptographisches Verfahren nach Anspruch 1 bis 3, dadurch gekennzeichnet, daß die Zahlen r und s im Bereich $[0, 2^k - 1]$ mit $16 \leq k \leq 32$ ausgewählt werden.

5. Kryptographisches Verfahren nach Anspruch 1 bis 4, dadurch gekennzeichnet, daß mindestens eine der Zahlen r und s so gewählt wird, daß die Binärdarstellung des Produktes $p \cdot r$ beziehungsweise $q \cdot s$ möglichst viele führende Einsen enthält.

6. Kryptographisches Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, daß beide Zahlen r und s so gewählt werden, daß die Binärdarstellung des Produktes $p \cdot r$ und des Produktes $q \cdot s$ möglichst viele führende Einsen enthalten.

7. Kryptographisches Verfahren nach einem der Ansprüche 5 oder 6, dadurch gekennzeichnet, daß

a) in einem ersten Teilschritt zunächst für mindestens eine der Zahlen r und s eine entsprechende optimale Zahl r_{opt} beziehungsweise s_{opt} ohne Beschränkung durch die Bedingung, gemäß der d teilerfremd zu $\phi(\text{lcm}(r,s))$ ist, ausgewählt wird, und

b) in einem zweiten Teilschritt jeweils ein benachbarter Wert $r = r_{opt} - i$ beziehungsweise $s = s_{opt} - i$, $i = 0, 1, \ldots, k$, ausgewählt wird, so daß d teilerfremd zu $\phi(\text{lcm}(r,s))$ ist.

8. Kryptographisches Verfahren nach einem der Ansprüche 5 oder 6, dadurch gekennzeichnet, daß

a) in einem ersten Teilschritt für jede der Zahlen r und s eine entsprechende optimale Zahl r_{opt} beziehungsweise s_{opt} ohne Beschränkung durch die Bedingung, gemäß der d teilerfremd zu $\phi(\text{lcm}(r,s))$ ist, ausgewählt wird, und

b) in einem zweiten Teilschritt jeweils ein Wert $r = 2^l \cdot r_{opt}$ beziehungsweise $s = 2^l \cdot s_{opt}$, $l = 0, 1, \ldots, j$, ausgewählt wird, so daß d teilerfremd zu $\phi(\text{lcm}(r,s))$ ist.

9. Kryptographisches Verfahren nach einem der Ansprüche 5 oder 6, dadurch gekennzeichnet, daß

a) in einem ersten Teilschritt mindestens eine der Zahlen r_{opt} und s_{opt} zunächst ohne Beschränkung durch die Bedingung, gemäß der d teilerfremd zu $\phi(\text{lcm}(r,s))$ ist, ausgewählt wird,

b) in einem zweiten Teilschritt jeweils ein benachbarter Wert $r = r_{opt} - i$ beziehungsweise $s = s_{opt} - i$, $i = 0, 1, \ldots, k$, ausgewählt wird, so daß d teilerfremd zu $\phi(\text{lcm}(r,s))$ ist, falls ein solcher Wert für $i = 0, 1, \ldots, k$ existiert, und

c) in einem dritten Teilschritt jeweils ein Wert $r = 2^i \cdot r_{opt}$ beziehungsweise $s = 2^i \cdot s_{opt}$, $i = 0, 1, \ldots, j$, ausgewählt wird, so daß d teilerfremd zu $\phi(lcm(r,s))$ ist, falls im zweiten Teilschritt kein Wert ausgewählt worden ist.

10. Kryptographisches Verfahren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß es das RSA-Verfahren beinhaltet.

11. Kryptographisches Verfahren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß es das Rabin'sche-Signaturen-Verfahren beinhaltet.

12. Kryptographisches Verfahren nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß es das Fiat-Shamir'sche Identifikationsschema-Verfahren beinhaltet.

13. Kryptographische Vorrichtung,

a) mit mindestens einer Exponentiationseinrichtung, die einen eine modulare Exponentiation E

$$E = x^d (\mathrm{mod}\ p \cdot q)$$

enthaltenden Rechenschritt mit einem ersten Primfaktor p, einem zweiten Primfaktor q, einem Exponenten d und einer Basis x ausführt, wobei

b) zur Durchführung der modularen Exponentiation zwei natürliche Zahlen r und s gewählt werden mit der Bedingung, daß d teilerfremd ist zu $\phi(lcm(r,s))$ und wobei die folgenden Rechenschritte durchgeführt werden:

$$x_1 = x(\mathrm{mod}\ p \cdot r)$$

$$x_2 = x(\mathrm{mod}\ q \cdot s)$$

$$d\_1 = d(\mathrm{mod}\ \phi(p \cdot r))$$

$$d\_2 = d(\mathrm{mod}\ \phi(q \cdot s))$$

$$z_1 = x_1^{d\_1}(\mathrm{mod}\ p \cdot r)$$

$$z_2 = x_2^{d\_2}(\mathrm{mod}\ q \cdot s),$$

und $\phi(.)$ die Euler'sche Funktion und lcm(r,s) das kleinste gemeinsame Vielfache von r und s darstellt,

c) anschließend nach dem Chinesischen Restwertsatz aus 21 und 22 eine Zahl z berechnet wird mit $z = z_1(\mathrm{mod}\ p \cdot r)$; $z = z_2(\mathrm{mod}\ q \cdot s)$

d) das Ergebnis E der Exponentiation durch Reduktion von z modulo $p \cdot q$ berechnet wird

e) die vorher berechnete Zahl z (und damit automatisch auch das Ergebnis E) in einem Prüfschritt auf Rechenfehler geprüft wird,

f) der Prüfschritt folgende Rechenoperationen beinhaltet:

f1) Berechnen der kleinstmöglichen natürlichen Zahl e mit der Eigenschaft $e \cdot d = 1 (\mathrm{mod}\ \phi(lcm(r,s)))$ mit Hilfe des erweiterten Euklid'schen Algorithmus

f2) Berechnen des Wertes $C = z^e(\mathrm{mod}\ lcm(r,s))$

f3) Vergleich der Werte x und C modulo lcm(r,s), wobei das Ergebnis der modularen Exponentiation E als fehlerhaft verworfen wird, wenn $x + C (\mathrm{mod}\ lcm(r,s))$.

14. Kryptographische Vorrichtung,

a) mit mindestens einer Exponentiationseinrichtung, die einen eine modulare Exponentiation E

$$E = x^d (\mathrm{mod}\ p \cdot q)$$

enthaltenden Rechenschritt mit einem ersten Primfaktor p, einem zweiten Primfaktor q, einem Exponenten d und einer Basis x ausführt, wobei

b) zur Durchführung der modularen Exponentiation zwei natürliche Zahlen r und s, sowie zwei Zahlen b_1 und b_2 im Intervall $[1, \ldots, r-1]$ bzw. $[1, \ldots, s-1]$ und teilerfremd zu r bzw. s gewählt werden, und wobei b_1 und b_2 die Bedingung $b_1 = b_2 (\mathrm{mod}\ ggt(r,s))$ erfüllen, wobei ggt(r,s) den größten gemeinsamen Teiler von r und s bezeichnet,

c) mit Hilfe dir beiden Zahlen b_1 und b_2 nach dem Chinesischen Restwertsatz Werte x_1 und x_2 berechnet werden, die die folgenden Bedingungen erfüllen:

$$x_1 = x(\mathrm{mod}\ p),\ x_1 = b_1(\mathrm{mod}\ r)$$

$$x_2 = x(\mathrm{mod}\ q),\ x_2 = b_2(\mathrm{mod}\ s)$$

und anschließend folgende Rechenschritte durchgeführt werden:

$$d\_1 = d(\mathrm{mod}\ \phi(p))$$

$$d\_2 = d(\mathrm{mod}\ \phi(q))$$

$$z_1 = x_1^{d\_1}(\mathrm{mod}\ p \cdot r)$$

$$z_2 = x_2^{d\_2}(\mathrm{mod}\ q \cdot s)$$

und wobei $\phi(.)$ die Euler'sche Funktion und lcm(r,s) das kleinste gemeinsame Vielfache von r und s darstellt,

d) anschließend nach dem Chinesischen Restwertsatz aus z_1 und z_2 eine Zahl z berechnet wird mit $z = z_1(\mathrm{mod}\ p \cdot r)$; $z = z_2(\mathrm{mod}\ q \cdot s)$;

e) das Ergebnis E der Exponentiation durch Reduktion von z modulo $p \cdot q$ berechnet wird

f) die vorher berechnete Zahl z (und damit automatisch auch das Ergebnis E) in einem Prüfschritt auf Rechenfehler geprüft wird,

g) der Prüfschritt folgende Rechenoperationen beinhaltet:

g1) Berechnen der Zahlen

$$C_1 = b_1^{d\_1}(\mathrm{mod}\ \cdot\ r)$$

$$C_2 = b_2^{d\_2}(\mathrm{mod}\ \cdot\ s)$$

wobei d_1 und d_2 vor der Durchführung der modularen Exponentiation modulo $\phi(r)$ bzw. $\phi(s)$ reduziert werden,

g2) Vergleich der Werte z_1 und C_1 modulo r sowie z_2 und C_2 modulo s, wobei das Ergebnis der modularen Exponentiation E als fehlerhaft verworfen wird, wenn $C_1 \neq z_1 \bmod r$ oder $C_2 \neq z_2 \bmod s$ gilt.

15. Kryptographische Vorrichtung nach Anspruch 14, dadurch gekennzeichnet, daß die Zahlen r und s ungerade sind.

16. Kryptographische Vorrichtung nach Anspruch 13 bis 15, dadurch gekennzeichnet, daß die Zahlen r und s im Bereich $\{0, 2^k - 1\}$ mit $16 \leq k \leq 32$ ausgewählt werden.

17. Kryptographische Vorrichtung nach Anspruch 13 bis 16, dadurch gekennzeichnet, daß mindestens eine

der Zahlen r und s so gewählt wird, daß die Binärdarstellung des Produktes $p \cdot r$ beziehungsweise $q \cdot s$ möglichst viele führende Einsen enthält.

18. Kryptographische Vorrichtung nach einem der Ansprüche 13 bis 17, dadurch gekennzeichnet, daß beide Zahlen r und s so gewählt werden, daß die Binärdarstellung des Produktes $p \cdot r$ und des Produktes $q \cdot s$ möglichst viele führende Einsen enthalten.

19. Kryptographische Vorrichtung nach einem der Ansprüche 17 oder 18, dadurch gekennzeichnet, daß

a) in einem ersten Teilschritt zunächst für mindestens eine der Zahlen r und s eine entsprechende optimale Zahl r_{opt} beziehungsweise s_{opt} ohne Beschränkung durch die Bedingung, gemäß der d teilerfremd zu $\phi(\text{lcm}(r,s))$ ist, ausgewählt wird, und

b) in einem zweiten Teilschritt jeweils ein benachbarter Wert $r = r_{opt} - i$ beziehungsweise $s = s_{opt} - i$, $i = 0, 1, \ldots, k$, ausgewählt wird, so daß d teilerfremd zu $\phi(\text{lcm}(r,s))$ ist.

20. Kryptographische Vorrichtung nach einem der Ansprüche 17 oder 18, dadurch gekennzeichnet, daß

a) in einem ersten Teilschritt für jede der Zahlen r und s eine entsprechende optimale Zahl r_{opt} beziehungsweise s_{opt} ohne Beschränkung durch die Bedingung, gemäß der d teilerfremd zu $\phi(\text{lcm}(r,s))$ ist, ausgewählt wird, und

b) in einem zweiten Teilschritt jeweils ein Wert $r = 2^l \cdot r_{opt}$ beziehungsweise $s = 2^l \cdot s_{opt} - i = 0, 1, \ldots, j$, ausgewählt wird, so daß d tellerfremd zu $\phi(\text{lcm}(r,s))$ ist.

21. Kryptographische Vorrichtung nach einem der Ansprüche 17 oder 18, dadurch gekennzeichnet, daß

a) in einem ersten Teilschritt mindestens eine der Zahlen r_{opt} und s_{opt} zunächst ohne Beschränkung durch die Bedingung, gemäß der d tellerfremd zu $\phi(\text{lcm}(r,s))$ ist, ausgewählt wird,

b) in einem zweiten Teilschritt jeweils ein benachbarter Wert $r = r_{opt} - i$ beziehungsweise $s = s_{opt} - i$, $i = 0, 1, \ldots, k$, ausgewählt wird, so daß d teilerfremd zu $\phi(\text{lcm}(r,s))$ ist, falls ein solcher Wert für $i = 0, 1, \ldots, k$ existiert, und

c) in einem dritten Teilschritt jeweils ein Wert $r = 2^l \cdot r_{opt}$ beziehungsweise $s = 2^l \cdot s_{opt}$, $i = 0, 1, \ldots, j$, ausgewählt wird, so daß d teilerfremd zu $\phi(\text{lcm}(r,s))$ ist, falls im zweiten Teilschritt kein Wert ausgewählt worden ist.

22. Kryptographische Vorrichtung nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß es das RSA-Verfahren beinhaltet.

23. Kryptographische Vorrichtung nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß es das Rabin'sche-Signaturen-Verfahren beinhaltet.

24. Kryptographische Vorrichtung nach einem der vorstehenden Ansprüche, dadurch gekennzeichnet, daß es das Fiat-Shamir'sche Identifikationsschema-Verfahren beinhaltet.

- Leerseite -